

Олександр Іщук  
Наталія Ніколаєва

**МЕТОДИ ЗАШИФРУВАННЯ  
КОРЕСПОНДЕНЦІЇ  
У ПІДПІЛЛІ ОУН І УПА  
ТА ЇХ РОЗШИФРУВАННЯ  
ОРГАНАМИ ДЕРЖАВНОЇ  
БЕЗПЕКИ УРСР  
В 1944-1954 рр.**



Київ - 2007

# ЗМІСТ

## ВСТУП

### 1. ЗАСТОСУВАННЯ КОДІВ

### 2. ЗАСТОСУВАННЯ ШИФРІВ

#### А) ПРОСТИЙ ШИФРУВАЛЬНИЙ КВАДРАТ

#### Б) СКЛАДНИЙ ШИФРУВАЛЬНИЙ КВАДРАТ

#### В) ШИФРУВАННЯ ЗА ДОПОМОГОЮ ПІДПІЛЬНОЇ ЛІТЕРАТУРИ

#### Г) ШИФРУВАННЯ ЦИФРОВИМ КЛЮЧЕМ

#### Д) ШИФРУВАННЯ ЗА ДОПОМОГОЮ ЗАМІНИ ЛІТЕР НА ІНШІ СИМВОЛИ

#### Е) ШИФРУВАЛЬНА РЕШІТКА

### 3. ТАЙНОПИС

## ВИСНОВКИ

## ІЛЮСТРАЦІЇ

У пропонованій книзі на основі архівних матеріалів органів державної безпеки УРСР та ОУН і УПА досліджуються методи зашифрування документів учасниками українського національно-визвольного руху. Особливу увагу у праці приділено вивченню методів розшифрування органами НКВС-НКДБ-МДБ-МВС-КДБ УРСР підпільних документів ОУН і УПА в 1944-1954 рр.

Книга призначена для дослідників історії України періоду Другої світової війни а також всіх, кого цікавить минуле нашої Батьківщини.

Відомості про авторів:

Іщук Олександр Степанович, кандидат історичних наук, старший науковий співробітник Галузевого державного архіву Служби безпеки України.

Школасва Наталія Борнсівна, кандидат історичних наук.

Якщо Вас зацікавила ця книжка, то з зауваженнями та пропозиціями Ви можете звертатись за тел 256-94-82 або 8(096)353-44-83.

## ВСТУП

Наше дослідження присвячене вивченню методів шифрування документів підпільниками Організації українських націоналістів (ОУН) і Української повстанської армії (УПА) в 1944-1954 рр. Його метою є на конкретних прикладах продемонструвати, якими методами користувалися підпільники ОУН, зашифровуючи свою кореспонденцію, і як ці записи намагалися розшифрувати органи державної безпеки УРСР.

На нашу думку, джерельна база дослідження є цілком достатньою. Збереглося багато архівних документів, в яких міститься інформація про застосування принципів конспірації в підпіллі ОУН і УПА. Вони викладені у брошурах „Конспірація”<sup>1</sup> (документ зберігся у кількох варіантах), „Конспірація та секрет”<sup>2</sup>, „Конспірація підпільника”<sup>3</sup>, „Конспіративний вишкіл”<sup>4</sup>, „Прийоми конспірації”<sup>5</sup> (автор – підпільник „М.Д.”), „Матеріали конспіративного вишколу”<sup>6</sup>, інструкціях „Конспіративна інструкція”<sup>7</sup>, „До відома всім членам і організаційним клітинам”<sup>8</sup> та інших<sup>9</sup>, які поширювалися серед підпільників ОУН у 1930-ті – 1940-ві рр. ХХ ст.

Слід відзначити, що задля більшої конспірації частина матеріалів про правила поведінки підпільників ОУН видавалися під виглядом брошур з сільського господарства і мали назви на кшталт „Сад і город”, Пашні буряки”, „Про хід ремонту тракторів” тощо<sup>10</sup>.

У вказаних документах подавалися основні принципи дотримання засад конспірації у підпіллі ОУН і УПА. В першу чергу, роз’яснювалися найголовніші положення:

- що таке конспірація, і для чого підпільникам потрібно постійно дотримуватися її вимог;
- як повинен себе поводити учасник ОУН і УПА, перебуваючи у підпіллі;
- як повинен себе поводити учасник ОУН і УПА, опинившись у людних місцях;
- як потрібно виявляти стеження поліції і як позбавитися від нього;
- як застосовувати принципи конспірації у повсякденному житті - поведінці, спілкуванні тощо;
- що таке підземні бункери, як їх потрібно будувати та як не допускати їх розконспірації;
- що таке організаційна каса та як її формувати та утримувати;
- як підпільники повинні проводити таємні зустрічі між собою;
- як здійснювати перехід через державний кордон;
- як організовувати та виконувати збройні акції;
- як потрібно себе поводити у випадку арешту, допитів, обшуків тощо.

У кожній брошурі з конспірації особлива увага приділялася застосуванню шифрів та кодів, принципи використання яких зазвичай викладалися у окремому розділі<sup>11</sup>. Безпосередньо з питань зашифрування

підпільних документів нами виявлені матеріали „Способи таємного порозуміння”<sup>12</sup>, „Ключ до шифру „рученька”<sup>13</sup> та інші<sup>14</sup>.

Цікава інформація про застосування принципів конспірації в листуванні між учасниками українського національно-визвольного руху міститься у опублікованих спогадах відомих підпільників – Р. Павленка<sup>15</sup>, М. Савчин<sup>16</sup> та інших.

Зовсім по-іншому виглядає науковий стан розробки проблеми. До 1991 р. проблема використання принципів конспірації піднімалася лише в окремих дослідженнях українських діаспорних істориків, оскільки представниками української радянської історіографії об’єктивного вивчення діяльності ОУН і УПА не проводилося. З 1991 по 2006 рр. у науковій літературі було опубліковано певний обсяг інформації про прийоми конспірації, які використовували підпільники ОУН, проводячи боротьбу за створення самостійної Української держави. Окремі згадки про них містяться у роботах А. Русначенка<sup>17</sup>, А. Кентія<sup>18</sup>, В. Сергійчука<sup>19</sup>, Д. Веденєєва<sup>20</sup>, в номерах 1-8 журналу „Український визвольний рух”, кількох томах серійного книжкового видання „Літопис УПА”<sup>21</sup> та інших виданнях.

Незважаючи на це, тема дослідження продовжує залишатися маловивченою українськими науковцями. Слід відзначити, що в українській науковій літературі і досі ще не з’явилось ґрунтовної праці, у якій би було проаналізовано всі методи зашифрування документів підпільниками ОУН і УПА. Зазвичай про шифри та коди у наукових працях згадується лише в контексті загального застосування підпільниками принципів конспірації. Авторам відомо про певні спроби окремих українських дослідників (зокрема, В. Мороза, І. Марчука, М. Романюка та інших) розшифрувати зашифровані записи ОУН і УПА. Прикладом можуть авторські розшифрування підпільних записів, вміщені у 8 томі нової серії „Літопису УПА”<sup>22</sup>.

Значний обсяг інформації про методи зашифрування документів у підпіллі ОУН міститься у документах радянських спецслужб, який нині зберігається у Галузевому державному архіві СБ України. У нашій праці ми спробуємо не лише охарактеризувати основні способи зашифрування документів в підпіллі ОУН і УПА, але й на конкретних прикладах продемонструвати методи їх розшифрування органами радянської держбезпеки.

\*\*\*

Учасники ОУН і УПА, проводячи свою підпільну роботу, намагалися щоденно дотримуватися вимог конспірації, аби не допустити провалу організаційних ланок. Зокрема, у організаційному листуванні їм необхідно було зашифрувати та закодувати важливу інформацію. Таким чином, шифрування кореспонденції було невід’ємною частиною принципів конспірації, які повсякденно застосовувалися підпіллям ОУН.

Підпільні організації підтримували контакти між собою лише за допомогою обумовлених способів зв’язку, повідомляючи про виконану

підпільну роботу, про зібрану на території інформацію, про свої подальші плани та наміри. Керівники підпільних структур ОУН часто надсилали вказівки у підпорядковані їм ланки виключно шифром. Вони добре розуміли, що без вміло організованого зв'язку та добре законспірованого листування підпільна робота проводиться нерационально, оскільки низові організації не можуть повідомити керівництву про результати здійсненої роботи, а керівництво в свою чергу не може проаналізувати зібрану інформацію та скерувати роботу у відповідне, необхідне на поточний момент, русло.

Зважаючи на вказане, підпільники приділяли функціонуванню законспірованих зв'язкових ліній виключну увагу. Вони розробили методику організації зашифрованого та закодованого листування, проводили спеціальні курси вишколу кадрів для оволодіння цими методиками. В першу чергу документація ОУН шифрувалася для того, щоб будь-які сторонні люди (як місцеві мешканці, так і працівники радянських органів влади) у разі захоплення підпільної пошти не могли нічого в ній зрозуміти.

На листах підпільників ніколи не було написано, кому саме адресується документ, а застосовувалися цифрові позначення адресата, тобто номер його поштової скриньки. Згідно із вимогами конспірації через певний час вони змінювалися. Наприклад, Головний командир УПА та керівник ОУН в Україні у 1943-1950 рр. Роман Шухевич у різний час використовував такі псевдоніми: „Тур”, „Тарас Чупринка”, „Шуб”, „Жар”, „Степан”, „Чернець”, „Туча”, „Білий”, „Мамай”, „Гриць”, „Чумак”, „Шух”, „Зайчик”, „777”, „205”, „315”, „171”, „553”<sup>23</sup>.

Керівник крайового проводу ОУН на Північно-західних українських землях Василь Галаса – „Орлан” у листуванні з підпільниками використовував різні псевдоніми:

З керівником ОУН і УПА в Україні Василем Куком – „Лемішем” – „515”, „Я”, „Ятер” і „Горпина”;

З керівником крайового проводу ОУН „Москва” Іваном Литвинчуком – „Дубовим” та керівником Рівненського окружного проводу ОУН Анатолієм Маєвським – „Ульяном” – „201”, „3248”;

З своїм заступником „38-А” – „Ф”, „ППШ”, „5x5”;

З підпільником „Максимом” – „5555” тощо<sup>24</sup>.

Так само різними псевдонімами підписували свої листи більшість керівників ОУН в Україні.

Таким чином слід визнати, що зв'язок є між підпільниками був найважливішою, але водночас і найбільш вразливою ланкою. Взагалі це стосується не лише діяльності ОУН, але й будь-якої нелегальної роботи.

З документів МДБ УРСР можна зробити висновок, що для припинення діяльності як українських націоналістів, так і інших супротивників радянської влади, спецслужбами в першу чергу здійснювалися намагання вклинитися у їх підпільні зв'язки з метою виявлення структури підпілля і його намірів. Саме тому співробітниками МДБ дуже велика, можна навіть сказати – величезна увага приділялася виявленню підпільних ліній зв'язків ОУН та розшифруванню підпільної пошти.

Підпілля ОУН застосовувало як прості, так і складні способи шифрування документів. Пошта ОУН в основному зашифровувалась за допомогою шифрів, кодів та тайнопису.

**Коди** – це умовна заміна визначальних слів і виразів на заздалегідь обумовлені слова, які в тексті не виділяються, однак для тих осіб, котрі знають код, повністю змінюють зміст написаного. Таким чином, при кодуванні відправником окремі слова та вислови замінювалися на інші, заздалегідь обумовлені, зрозумілі лише отримувачу. Зазвичай закодований текст ззовні має цілком звичайний характер, і якщо не вдумуватися у його зміст, то його нічим не можна відрізнити від звичайного побутового листування.

Закодованим листуванням часто користувалися легальні прихильники ОУН для листування між собою, оскільки вони були переконані, що їх листи не контролюються радянською контррозвідкою.

**Шифри** – це зовсім інший спосіб листування. При його використанні кожна літера, а іноді і кожен знак пунктуації, замінювалися на іншу літеру, цифру або інші умовні знаки. Іноді букви не замінюються на інші, але записувалися у відповідному порядку, що унеможливило нормальне прочитання написаного тексту.

Підпільники ОУН в залежності від обставин зашифровували як цілі листи, так і їх окремі фрагменти, які бажали зберегти у таємниці.

Зашифрований текст можна було виявити одразу, оскільки він виділявся на фоні іншого (незашифрованого) тексту наявністю груп цифр, незрозумілим набором літер та значків у нестандартному порядку. Однак він значно важче піддався розшифруванню, ніж код. Часто бувало так, що у разі незначної кількості зашифрованих слів у листі співробітники МДБ не мали за що зачепитися, щоб розшифрувати підпільного листа, і його подальше дешифрування було практично неможливим.

Частіше за все різноманітні зашифровані тексти зустрічалися у листуванні між собою керівників ОУН. Ці листи переносили підпільні кур'єри на лініях нелегального зв'язку від одного керівника або проводу до іншого. Зазвичай підпільна пошта передавалася у вигляді „грипсів” (вони ж мали назву „штафети”) – листів, написаних на тонкому цигарковому папері дрібними літерами, щільно загорнутих у невеликий компактний пакетик величиною не більше третини стандартної цигарки.

Підпільники ОУН зазвичай використовували шифри під час укладання списків осіб, які матеріально допомагали підпіллю, утримувачів конспіративних квартир та бункерів ОУН, молоді, легально проживаючих людей. Крім того зашифровувались місця зберігання зброї, набоїв, літератури, продуктів харчування, одягу та іншого майна.

Керівники підпілля ОУН у своїх особистих блокнотах також зашифровували найбільш важливі записи (зв'язки до інших підпільників, особисті біографічні дані, дані про рідних, підлеглих і т.п.), щоб у випадку смерті і вилучення записів співробітниками органів держбезпеки УРСР ніхто не постраждав.

Звісно, що своєчасне дешифрування листів та інших документів учасників ОУН давала в руки МДБ цінну інформацію, яка використовувалася під час знищення підпілля.

У Галузевому державному архіві СБ України збереглася інформація про виявлення та дешифрування документів ОУН, які потрапили до співробітників МДБ. Їх використання дало можливість радянським органам державної безпеки провести успішні заходи проти підпілля ОУН.

## 1. ЗАСТОСУВАННЯ КОДІВ.

Під час ліквідації співробітниками МДБ у серпні-вересні 1947 р. в Луцькому та сусідніх із ним районах Волинської області боївки ОУН мельниківського напрямку, яку очолював „Похмурий”, був вилучений код, складений за кордоном. „Похмурий” працював в Україні за завданням закордонного керівництва ОУН(м) та повинен був інформувати його про ситуацію в Україні за допомогою спеціального коду, з яким були ознайомлені лише довірені особи. Після отримання інформації вони за допомогою коду зашифровували інформацію та надсилали її у звичайних листах на заздалегідь обумовлені адреси за кордон. У листуванні між собою підпільники також повинні були користуватися вказаним кодом.

Ось деякі слова та їх зашифрування із цього коду:

Організація = шкільний курс,

Округ = місцевий гурток,

Член (друг) = професор,

Член (подруга) = відмінник,

Організаційна література = ягода,

Розвідка = квіти,

Сибір = Славка,

Зв'язок = пейзаж,

Зрадник = зозуля,

Провокатор = соловей,

Видати = редакція,

Тюрма = розрахунок,

Документи = подруга,

Пункт = клуб,

Підпілля = дорога,

Інформація = життя і т.д.

Як використовувався цей код можна побачити з простого прикладу. Припустимо, що хтось із підпільників вирішив написати своєму керівнику лист наступного змісту:

„... Я встановив, що організація продовжує діяти, але окружний провід не має достатньо членів для проведення розвідки і розповсюдження літератури. Три члена і одна подруга потрапили в тюрму і їм може загрожувати вивіз у Сибір. Провокаторів поки що не виявили, але є один

зрадник. Він видав двох членів і пункт з документами. Інформація надходить погано...”.

Всі підкреслені слова необхідно було закодувати, оскільки якщо їх залишити у тексті, то це викликало б підозру. Після закодування вказаний вище текст мав би наступний вигляд:

„...Я дізнався, що шкільний курс продовжує роботу, але в місцевому гуртку не вистачає професорів із розведення квітів та збору ягід. Три професора та один відмінник з місцевих отримали розрахунок і, судячи з усього, поїдуть в гості до Славки. Був у лісі, солов'їв не чути, але чув зозулю. Редакція бере на роботу двох професорів, їх подруги влаштовуються у клубі. Так що життя погане...”.

Як бачимо, в результаті закодування вийшов цілком звичайний і нічим не примітний текст. Водночас у ньому зашифрована важлива інформація.

Слід відзначити, що при уважному вивченні листів співробітники МДБ виявляли закодований текст, оскільки в окремих його місцях зустрічалися не зовсім правильні граматичні конструкції, в інших – не було чіткої логічної послідовності, і взагалі відчувалося перескакування з однієї теми на іншу. Але при уважному використанні коду та правильному складанні тексту підпільники уникали непослідовності і склали настільки вивірені тексти, що їх практично неможливо було розшифрувати<sup>25</sup>.

Окрім вказаного способу закодування текстів, учасники ОУН у своїх листах намагалися закодувати час і місце зустрічі, наперед обумовлювали між собою необхідні паролі для їх проведення.

14 травня 1953 р. у вбитого керівника Луцького окружного проводу ОУН Олександра Савири - „Яроша” було вилучено код, який він використовував для призначення підпільних зустрічей:

„... час – задача + 12, ярлик + 3, число дня – трудоднів + 30, місяць – остаток рублів + 170.

Ліс – сторінки:

Боголюбський – 2,

Голятинський – 6,

Завидівський – 11,

Коритницький – 13,

Ківерцівський – 17,

Ульяницький – 32,

Фусівський – 33.

Область – глава книги.

Волинь – I,

Рівненська – II,

Львівська – IV,

Тернопільська – VI,

Київська – XI,

Полтавська – XIII,

Донбас – XIV.

Район – кількість членів тракторної бригади.



Рожище – 1,  
 Затурці – 2,  
 Колки – 10,  
 Голоби – 11,  
 Горохів – 14,  
 Радехів – 17,  
 Іваничі – 19,  
 Володимир-Волинський – 21,  
 Устилуг – 22.  
**Місто - % міцності вина + 20.**  
 Львів – 1,  
 Радехів – 2,  
 Дубно – 5,  
 Ковель – 9,  
 Луцьк – 10,  
 Київ – 15,  
 Москва – 21...” і т.д.

Як же О. Савира використовував цей код?

Співробітниками МДБ було встановлено, що код використовувався для призначення місця зустрічі як з підпільниками, так і з легальними прихильниками ОУН.

Припустимо, зустріч призначалася на 20 травня о 21 год. 30 хв. у Завидівському лісі Іваничівського району Волинської області (або в м. Дубно). Це можна було зашифрувати наступним чином: „Донька не може вирішити задачу № 33. Я відпрацював вже 50 трудоднів, все ще винний сусіду 175 рублів, але скоро розрахуюсь. Я читаю твою книгу, мне сподобалась 11 сторінка, 1 глава. В нашій тракторній бригаді вже працює 19 людей (або: у вині, яке я зробив, міцність всього 25%)”.

Звісно, що підпільники підбирали довільний текст для таких листів, а головним у них були цифри та слова, які були закодовані<sup>26</sup>.

Своєчасне розшифрування подібних документів ОУН неодноразово допомагало співробітникам МДБ проводити успішні операції.

4 листопада 1949 р. співробітниками Управління МДБ по Волинській області був вбитий організаційний референт крайового проводу ОУН на Північно-західних українських землях Андрій Неверковець - „Хома”, він же „Ілько”, „Ган” і „Прокіп”<sup>27</sup>. У нього було вилучено значну кількість документів, в тому числі – його особисті записники. У них було знайдено записи про те, що 14-15 і 20-21 листопада 1949 р. А. Неверковець мав зустрітися з іншими керівниками на умовних пунктах „Бджола”, „Молот”, „Розсоха”, № 2 та № 4. Поруч були вказані пвролі, необхідні для зустрічі.

Надаючи велике значення виявленню точного місця зустрічі керівників підпілля, співробітники УМДБ по Волинській області ретельно переглянули та проаналізували всі захоплені у А. Неверковця документи. В результаті їм вдалося розкодувати, що словом „Бджола” умовно називався Коритницький

ліс, розташований на адміністративному кордоні Горохівського та Локачинського районів Волинської області.

У зв'язку з тим, що конкретні місця зустрічі співробітникам МДБ були не відомі, 10 листопада 1949 р. у Коритницький ліс було таємно викинуто кілька пошукових груп, які склалися із колишніх підпільників ОУН. Вони раніше неодноразово бували в цьому лісі, і тому заздалегідь відмітили 7 найбільш ймовірних місць, де могли б зустрітися підпільники.

12 листопада 1949 р. біля всіх цих пунктів були висаджені засади, які були ознайомлені з паролями, вилученими у І. Неверковця.

В ніч на 21 листопада 1949 р. приблизно в 200 метрах від однієї із засад військовослужбовці почули умовний сигнал. Чекістсько-військова група, подаючи сигнал у відповідь, підкликала підпільника на близьку до себе відстань. Однак він виявився обережним і не підійшов настільки близько, щоб його можна було спробувати захопити живим. У зв'язку з цим його убили. Підпільником виявився кур'єр крайового проводу ОУН на Північно-західних українських землях „Роман”, у якого було вилучено дуже цінні документи підпілля на адресу керівників ОУН в Західній Україні.

Таким чином, завдяки своєчасному та точному розкодуванню документів оперативникам МДБ вдалося перервати лінію зв'язку крайового проводу ОУН на Північно-західних українських землях та отримати важливі документи<sup>28</sup>.

Підпільні коди активно використовували Василь Кук – „Леміш”, Василь Охрімович – „Грузин”, Василь Галаса – „Орлан” та інші керівники підпілля ОУН.

## 2. ЗАСТОСУВАННЯ ШИФРІВ.

### А) Простий шифрувальний квадрат.

При шифруванні всі літери у словах замінювались за визначеною системою на інші букви, цифри і знаки або ж розташовувались у тексті у відповідному порядку, щоб його прочитання без знання всіх умовностей (ключа) ставало неможливим.

Найпростішим способом шифрування у підпільників ОУН було застосування так званого шифрувального квадрату. Цей метод шифрування полягає у тому, що всі літери алфавіту, а іноді і знаки пунктуації, вписувалися у квадрат, розділений на горизонтальні та вертикальні рядки. Вертикальні рядки нумерувалися зліва направо, а горизонтальні – згори донизу.

Якщо необхідно було зашифрувати літеру, то її шукали в квадраті, визначали, де вона знаходиться і замість неї писали дві цифри: першу – номер горизонтального рядка, і другу – номер вертикального рядка.

Цей спосіб шифрування використовувався багатьма підпільниками, як в Галичині, так і на Волині.

15 грудня 1948 р. в с. Бояри Брестської області Білоруської РСР було вбито кілька учасників ОУН, які діяли у складі Брестського (або Білоруського, як його ще називали) окружного проводу ОУН. У них було захоплено багато документів, і серед них – обліковий листок на члена ОУН за псевдонімом „Григор”, який в підпіллі виконував обов’язки організаційного референта Білоруського окружного проводу ОУН. Не знаючи дійсних установочних даних на „Григора”, керівники УМДБ по Брестській області БРСР направили фотокопію цього документу в УМДБ по Волинській області УРСР для розшифрування.

Уривок цього облікового листка мав такий вигляд:

**Псевдо: Григор.**

**Прізвище та ім’я: 73 15 74 51 65 74 13 23 43 55 54 12 43 74 42 41 55 45  
55 41 12 62 55 33.**

**Місце народження:**

**51 14 45 12 42 24 43 74 15 44 73 12 62 74 45 23 44 23 11 12 61 12 15 14  
42 12 13 32 43 74 15 13 12 41 64 45 23 44 23 11 12 53 12 73 45 14 44 43 64.**

Проаналізувавши цей зашифрований запис, співробітники УМДБ по Волинській області зробили висновок, що шифрування було здійснено по квадрату. Це підтверджувалося тим, що хоча всі цифри ідуть підряд, але цифра більше 7 не зустрічається, а саме в квадратах кількість рядків береться не більше 7-9. Окрім того, в тексті була парна кількість чисел: перша могла означати горизонтальні, а друга – вертикальні рядки квадрату. Не було в тексті і двохзначних цифр, інакше їх неможливо було б виділити.

Приступивши до дешифровки, співробітники УМДБ по Волинській області в першу чергу спробували розшифрувати закінчення слів. У даному випадку вони мали на увазі те, що в графі „прізвище та ім’я”, мабуть, було зашифроване і по-батькові підпільника, оскільки в тексті було аж 24 цифри. В українській мові майже завжди по-батькові має закінчення „вич” – так було висловлено здогадку про три літери.

Далі оперативники припустили, що грамотні люди разом із роком народження зазвичай потім пишуть місто або село, потім район, а потім – область. Чекісти знали, що „Григор” мав середню освіту. Отже, в кінці запису мало стояти слово „області”.

Під час дешифрування цього запису оперативники пам’ятали, що в українській мові є найбільш вживані літери, і вони завжди зустрічаються в тексті частіше за інші. Оскільки у цьому шифрі кожна літера мала лише одне цифрове позначення, то оперативники виділили вказані цифри.

Підставивши здогадувані букви у шифрований текст, оперативники знайшли знайомі слова, у яких бракувало по кілька літер. Так поступово вони встановили весь шифр. Систематизувавши всі літери та їх числові

позначення, які стали відомі, оперативники склали ключ до даного шифру, який мав такий вигляд:

	1	2	3	4	5	6
1	К	О	Н	А	Р	
2		4	Ь	Я	Е	
3	З	У	Ч	Х	Щ	Ю
4	П	Й	Т	С	Л	
5	З	Ж	Ї	М	И	І
6	Г	В	Ф	І	Д	
7	Ш	Ц	Б	Е		

Скориставшись цим ключем, оперативники розшифрували весь текст облікової картки і отримали такий результат:

**Прізвище та ім'я:** Брездень Тимотей Пилипович.

**Місце народження:** Залоя, Терсбовельського району Тернопільської області.

У цьому тексті при зашифруванні підпільники зробили помилки. Назви села і району написані невірно: „Залоя” замість „Залав'є”, „Терсбовельського” замість „Теребовельського”. Це і не дивно. Вказаний ключ було важко запам'ятати, його потрібно було постійно мати при собі записаним на папері<sup>29</sup>.

Щоб полегшити запам'ятовування шифру, підпільники ОУН іноді користувалися таким способом: вибирали одне слово, щоб його букви рівномірно розподілялися по всьому українському алфавіту і, написавши його в квадрат у верхній горизонтальний рядок, від кожної літери продовжували алфавіт вниз. При цьому слід відзначити, що оскільки на той час існувало кілька варіантів українського алфавіту, то підпільники домовлялися використовувати один із них.

Наприклад, ключовий словом вибрали слово „конашевич”. Тоді шифрувальний квадрат матиме такий вигляд:

	1	2	3	4	5	6	7	8	9
1	К	О	Н	А	Ш	Е	В	И	Ч
2	Л	П	О	Б	Щ	Є	Г	Й	Ш
3	М	Р	П	В	Ю	Ж	Д	Ї	Щ
4	Н	С	Р	Г	Я	З	Е	К	Ю
5	О	Т	С	Д	Ь	І	Є	Л	Я
6	П	У	Т	Е	А	И	Ж	М	Ь
7	Р	Ф	У	Є	Б	Й	З	Н	А
8	С	Х	Ф	Ж	В	Ї	І	О	Б
9	Т	Ц	Х	З	Г	К	И	П	В

Такий квадрат запам'ятати легше, оскільки потрібно знати лише одне слово, від якого будується шифр. Зашифрування за цим квадратом здійснювалося за тим же принципом, як і за попереднім<sup>30</sup>.

### Б) Складний шифрувальний квадрат.

В підпіллі ОУН використовувалися і більш складні шифрувальні квадрати.

У листопаді 1950 р. у 2 Головному управлінні МДБ СРСР було вивчено комбінований шифрувальний квадрат, вилучений у підпільників ОУН. Квадрат мав 10 горизонтальних та вертикальних рядків, причому в нього були вписані всі цифри від 0 до 9 та два українських алфавіти (навіть з російськими літерами!) від „а” до „я” (всього 66 літер):

	А	Б	В	Г	Д	Е	Ж	З	И	К								
	1	2	3	4	5	6	7	8	9	0								
1	А	Б	В	Й	Г	Д	Е	З	Ж	И	1	К						
2	І	К	Л	М	Н	О	П	Р	С	Т	2	Л						
3	Ф	Х	Ц	Ч	Ш	Щ	Є	Ь	Ю	Я	Ы	Ї	У	3	М			
4							1	2	3	4	5	6	7	8	9	0	4	О
5	Э	Ъ		Т	І	Р	З	В	С	У							5	П
6	Є	Ч	Г														6	С
7	Ю	К	Ж	И	М	Н	О	Й	,	;	!	?					7	Т
8	Х		Л					Ї	.	:	□						8	У
9	Ш	Щ	Ц	α	□	Е	Д	П	„	*	)	(					9	А
0	Ь	Я	Б					Ф	∪	□	□						0	Б
	1	2	3	4	5	6	7	8	9	0								
	А	Б	В	Г	Д	Е	Ж	З	И	К								

Як бачимо, цей шифрувальний квадрат навіть ззовні виглядає складнішим, ніж попередні.

По-перше, він пронумерований літерами та цифрами з усіх чотирьох боків: згори, знизу, зліва і справа.

По-друге, в ньому є пунктуаційні знаки („\*“, „( )“, „;“, „:“, „?“ тощо), геометричні фігури та грецькі літери, вживані в математиці („α“, „∪“, „□“).

По-третє, літери і цифри в квадраті розташовані нерівномірно. Деякі клітини квадрату містять одну букву, інші розбиті на дві рівні частини, в кожену з яких вписані окремі літери та цифри. Окрім того, кілька літер вписані в клітини, об'єднані з двох стандартних клітин.

По-четверте, кілька клітин у квадраті взагалі порожні.

За висновками дешифрувальників, у цьому квадраті було вміщено неповний ключ шифру, який складався із величин, які потрібно було зашифрувати.

Принцип шифрування документів за вказаним шифрувальним квадратом полягав у тому, що кожна літера українського алфавіту, яку потрібно було зашифрувати, відшукувалася у квадраті. Після цього, в залежності від того, як було заздалегідь обумовлено, визначалися координати за якими вона розташовувалася, і вносилися у зашифрований текст у вигляді цифр або літер. Наприклад, шифруємо цифрами, спочатку по вертикалі зліва, потім по горизонталі згори; буквами – спочатку по вертикалі справа, потім по горизонталі знизу.

В цьому випадку, якщо підпільникам потрібно було зашифрувати слова „наша держава”, після використання шифрувального квадрату вони мали такий вигляд:

Слова, які треба зашифрувати	Н	А	Ш	А	Д	Е	Р	Ж	А	В	А
Цифровий шифр	25	11	91	11	16	61	28	73	11	13	11
Буквений шифр	ЛД	КА	АА	КА	КЕ	КЖ	ЛЗ	ТВ	КА	КВ	КА

Всі цифри і літери вносяться у шифрувальний текст без пунктуаційних знаків, оскільки вони також шифруються.

Цікаво, що чекісти до кінця не розібрались в тому, як підпільники використовували цей квадрат, зокрема клітини, розбиті на дві частини. Проте можна припустити, що для них було обумовлено якесь позначення. Наприклад, щоб зашифрувати знак „\*” (буквами – спочатку по вертикалі справа, потім по горизонталі знизу) могли використати дріб: „аи/2”. Це означало, що знак „\*” знаходиться у другій частині розбитої навпіл клітини.

Розшифрування здійснювалося у зворотному порядку. За вказаними координатами у шифрувальному квадраті відшукувалися потрібні літери<sup>31</sup>.

### **В) Шифрування за допомогою підпільної літератури.**

Ще одним дуже поширеним способом у підпільників ОУН було зашифрування листування за допомогою підпільної літератури

Для використання цього способу підпільники домовлялися між собою за якою брошурою або листівкою вони будуть зашифровувати текст. Потім визначали у тексті сторінку, абзац, рядок і потрібну букву, яку позначали цифровим дробом, у якому чисельник вказував на номер рядка згори сторінки, а знаменник – на номер букви у рядку, починаючи зліва.

Для зашифрування цифр у цьому випадку бралася слово із 10 літер, в якому літери не повторювалися, і кожна з них в ньому позначалася зліва направо від 1 до 10. Цими літерами користувалися для вказування цифрових позначень.

Як саме виглядав такий шифр видно із конкретного прикладу. В січні 1953 р. з повинною до органів МДБ вийшов бойовик Луцького окружного провідника О. Савири - „Яроша” підпільник „Тарас”. За його свідченнями в с. Колодеже Сенкевичівського району Волинської області було виявлено

бункер, де зберігалася значна кількість документів та літератури ОУН, зокрема – записи керівників Луцького округу. Серед останніх було виявлено аркуш із зашифрованими записами, де, судячи з усього, вказувалися люди, які співробітничали з підпіллям ОУН у різних селах Волинської області. Один із цих записів мав такий вигляд:

**½ 2/2 9/1 2/11 2/12 6/2.**

**¾ 2/4 6/1 6/2 3/1 2/5 9/1.**

**½ 2/2 1/14 2/2 ½ 2/2 1/1 1/6 2/2.**

**11/5 4/2 ¾ 1/1 1/13 ½ 1/3 9/1.**

**4/2 2/5 6/2**

**½ 2/2 4/2 к д к о 3/1 6/1 1/12 ¾.**

**2/11 2/2 4/2 5/4 6/2 2/5 1/6.**

**4/2 8/8 ½**

**3/1 6/1 ½ 6/2 6/1 1/6 1/3 2/11 2/5 1/6 3/1 1/13 6/2 1/3 9/1.**

**Я козак із Запоріжжя.**

**А я волинський хлібороб.**

**КО – ОА**

Окрім того у документі було ще 5 схожих записів.

З чого ж співробітники МДБ розпочинали розшифрування таких документів?

В першу чергу вони відзначили, що останні три речення у записі – це пароль та зашифровані дати зустрічей. Ймовірно, що підпільник, який мав зустрітися із цим прихильником ОУН, спочатку мав привітатися з ним словами „Я козак із Запоріжжя”, на що отримати відповідь „А я волинський хлібороб”.

Далі співробітники МДБ намагалися визначити, за якою саме системою було проведено зашифровку. Вивчивши уважно всі цифри в шифрі вони переконалися, що серед них зустрічаються двозначні, такі, як 11, 12, 13, 14 і т.д. Це підтверджувало те, що зашифрування проводилося не по шифрувальному квадрату, у якому кількість горизонтальних та вертикальних рядків зазвичай не перевищує 7-9. Двозначні цифри наводили на думку про те, що зашифровка була здійснена за одним із найулюбленіших способів підпільників – за брошурою або листівкою.

Чекістам було відомо про те, що керівник Луцького окружного проводу О. Савира – „Ярош” і його бойовики діяли виключно на території Волинської області, і крім неї їх бачили тільки в Демидівському районі Рівненської області. Проаналізувавши інші вилучені документи, оперативники склали їх повний список, відмітили різні умовні позначення, з’ясували, які боївки передавали звіти „Ярошу”, приблизну територію дій підлеглих „Яроша” (райони, села, хутори), вивчили інші зашифровані документи, які були захоплені на цих територіях. З’ясування всіх цих питань полегшило розшифрування документів.

Зіставивши всю зібрану інформацію, співробітники МДБ дійшли до таких висновків:

1. На початку кожного із шести записів стоять порівняно невеликі слова, які можуть означати прізвища та імена. В Західній Україні більшість українських прізвищ закінчується літами „ук” або „юк” (наприклад, Власюк, Шумук). Виходячи з цього дріб 6/2 (закінчення першого слова) гіпотетично означили, як літеру „к”.

2. Майже кожен запис у документі закінчувався однаковими цифрами, що дало підстави вважати їх закінченнями аналогічних слів. Такими словами могли бути назви районів Волинської області. Назви районів українською мовою майже завжди закінчуються на „ський” або „цький” (наприклад Торчинський, Луцький). Ця гіпотеза підтверджувалася ще й тим, що третьою літерою ззаду стоїть цифрове позначення 6/2, що за першим припущенням позначає літеру „к”.

3. Таким чином, за припущеннями співробітників МДБ, стало відомо кілька літер: 3/1 = с; 6/2 = к; 1/3 = и; 9/1 = й.

Підставивши їх у зашифровані прізвища та імена прихильників ОУН, можна здогадатися і про інші літери.

У цьому випадку співробітники МДБ поставили зазначені літери в один із блоків цифр, і отримали напіврозуміле слово:

¾ 2/4 6/1 к с 2/5 й

Тут вже неважко було здогадатися, що розшифровкою могло бути ім'я „Олексій”.

4. Після цього вже вистачило справжніх літер, щоб вставити їх у зашифрований текст і розшифрувати весь запис. Отриманий результат був таким:

**Найчук Олексій, наша назва Грозьний, рік нар. к д к о, село Чаруків, район Сенкевичівський.**

**Я козак із Запоріжжя. А я волинський хлібороб.**

**КО – ОА.**

5. В кінці чекісти зайнялись розшифруванням літер, якими, судячи з усього, зашифрували цифри. Судячи із змісту запису, літери „кдко” мали означати рік народження особи. За логікою, він повинен розпочинатися з цифр „19...”, а оскільки третя літера така сама, як перша, то можна припустити, що прихильник ОУН був 191(?) року народження. Прихильниками ОУН в основному була молодь, та й взагалі важко було припустити, що підпіллю допомагала особа 181(?) р.н., адже люди так довго не живуть

Згодом, після розшифрування всіх цифр, які були в шести записах в документі, було встановлено, що вони були зашифровані словом „колесаниду”, в якому кожна літера означала певну цифру (к – 1, о – 2, л – 3, е – 4 і т.д.). Таким чином, О. Найчук був 1912 р.н.



У записі про О. Найчука в кінці вказувалися літери „КО - ОА”. Ймовірно ними були зашифровані щомісячні дати зустрічей Найчука із підпільниками ОУН. Звірівши літери з словом „колесаніду” чекісти отримали дві дати зустрічей – 12 і 26 числа кожного місяця.

Таким чином, співробітники УМДБ по Волинській області здійснили повну розшифровку вказаного тексту. Однак на цьому робота дешифрувальника не закінчувалася. Ще необхідно було з'ясувати, за якою брошурою або листівкою було проведено зашифровку, щоб згодом у разі захоплення інших зашифрованих документів не витратити час на розшифровку а одразу ж прочитати текст.

Після тривалої перевірки співробітники УМДБ по Волинській області встановили, що у даному випадку зашифрування тексту було здійснене за восьмою сторінкою брошури ОУН „Поневолений український народ!”. Причому для ускладнення розшифрування документа текст цієї сторінки брошури був розділений між словами приблизно навіпіл розмежувальною лінією. Безпосередньо для зашифрування використовувався текст правіше від розмежувальної лінії (дивись ілюстрацію).

Характерно відзначити, що розшифрований документ допоміг співробітникам МДБ у боротьбі з підпільниками. За виявленими прихильниками ОУН було встановлено нагляд, проаналізовано місцезнаходження їх будинків та навколишньої місцевості. В результаті узагальнення всіх даних було зроблено припущення, що у одного з розшифрованих осіб може знаходитися бункер ОУН. Під час обшуків та перевірок це припущення виправдалося<sup>32</sup>.

### Г) Шифрування цифровим ключем.

Зовсім інший принцип шифрування, який застосовувався підпільниками ОУН, називався шифруванням цифровим ключем.

Для цієї зашифровки тексту перш за все вибирався цифровий ключ з будь-якого набору цифр, але такий, щоб його можна було легко запам'ятати. Зазвичай підпільники вибирали дату народження чи смерті якого-небудь українського громадського чи політичного діяча, вченого, письменника і т.д. В основу шифрування закладався порядок розташування літер українського алфавіту. До тексту, який планується зашифрувати, підставлявся ключ. Цифра ключа додавалася до цифри, яка відповідає місцю розташування шифрованої літери в українському алфавіті. У шифрованому тексті ставилася та літера, яка містилася у алфавіті під номером, який був сумою вказаних чисел.

Цей спосіб шифрування був доволі складним, але виправдовував себе тим, що і розшифрувати його не так просто, оскільки одна та ж сама літера шифрованого тексту може означати різні літери дійсного тексту. Для ускладнення розшифрування підпільники ОУН іноді не шифрували окремі літери і вносили їх в текст в обумовленому порядку.

Для пояснення цього способу шифрування наведемо конкретний приклад.

У 1947 р. УМДБ по Волинській області здійснювало активний розшук крайового проводу ОУН „Москва”, яким керував Іван Литвинчук – „Максим Дубовий”. В той час оперативникам не були відомі справжні прізвища та імена кількох функціонерів цього проводу, чим гальмувався їх розшук.

При проведенні однієї з чекістсько-військових операцій в с. Боголюби Луцького району Волинської області був виявлений та відкритий бункер ОУН, в якому конфісковано значну кількість підпільної літератур, записів та блокнотів. У їх числі були вилучені кілька евіденційних листків - так у підпіллі називалися листки обліку кадрів. У цих документах згори були написані псевдоніми підпільників, а вся інша інформація була зашифрована невідомим літерним шифром, тобто замість змістовного тексту стояв набір букв.

Співробітники УМДБ по Волинській області шляхом ретельного вивчення та аналізу тексту, співставлення окремих слів, їх закінчень, гіпотетичної підстановки слів та літер з'ясували, що ключем для зашифрування вказаного тексту була цифра 931814, тобто дата народження українського поета Тараса Шевченка – 9 березня 1814 року.

Зашифрування тексту здійснювалося наступним чином.

Припустимо, що підпільникам потрібно було зашифрувати слова „Слава Україні”. Для цього за українським алфавітом брався порядковий номер кожної літери (наприклад, с – 21, л – 15, а – 1 і т.д.), потім цифри сплюсовувалися з шифрувальним ключем. За отриманою цифрою із українського алфавіту бралася літера, яка і вписувалася у документ:

Слова, які потрібно зашифрувати	С	Л	А	В	А	У	К	Р	А	Ї	Н	І
№ літер в українському алфавіті	21	15	1	3	1	23	14	20	1	12	17	11
Шифрувальний ключ	9	3	1	8	1	4	-	9	3	1	8	1
Сума	30	18	2	11	2	27	-	29	4	13	25	12
Літера, яка в українському алфавіті відповідає цифрі суми	Ю	О	Б	І	Б	Ч	К	Щ	Г	Й	Х	Ї

Як бачимо, в результаті шифрування утворився набір нічого не означаючих літер. Слід відзначити, що літера „к” у слові „Україні” не шифрувалася, що було обумовлено підпільниками наперед для ускладнення розшифровки документу<sup>33</sup>.

Якщо підпільники ОУН отримані таким чином літери ще раз зашифровували за допомогою описаного вище простого шифрувального квадрату, то розшифрувати такі документи було практично неможливо.

Більш простим способом, який використовували вояки УПА, було використання невеликого цифрового ключа, зазвичай із 3-4 цифр. 3 лютого

1946 р. співробітники МДБ у пустому бункері неподалік одного з сіл Жовківського району Львівської області виявили зашифровані документи УПА і цифровий код до них – „1243”.

Шифрування документів відбувалося наступним чином. Припустимо, що підпільникам потрібно було зашифрувати фразу „Сорока виїхав у село Майдан”. Вони писали її на папері, а під кожною літерою – цифри із ключа.

Шифр передбачав, що замість кожної літери, під якою написана цифра, необхідно написати одну із наступних літер українського алфавіту, а саме ту літеру, яка стоїть вправо на відстань, вказану цифрою кодового ключа

Наприклад: замість першої літери фрази – „с” підпільники писали наступну літеру алфавіту вправо, тобто літеру „т”. Замість другої літери – „о” писали другу літеру вправо від неї в алфавіті, тобто „р” і так далі:

с	о	р	о	к	а	в	и	ї	х	а	в	у	с	е	л	о	м	а	й	д	а	н
1	2	4	3	1	2	4	3	1	2	4	3	1	2	4	3	1	2	4	3	1	2	4
Т	Р	Ф	С	Л	В	Е	Й	І	Ч	Г	Д	Ф	У	И	С	П	О	Г	М	Е	В	С

В результаті зашифрування фрази підпільники отримували наступний, незрозумілий для сторонніх осіб, набір літер: **трфслв ейічгд фуисп огмевс** (оскільки учасники ОУН використовували справжню, а не радянську граматику, то літера „г” в даному вигляді матиме вигляд „найбільш української літери” - „г”).

Розшифрування документів здійснювалося у зворотному порядку за допомогою того ж цифрового ключа.

Окремо слід відзначити, що підпільники іноді зазначали у своїх донесеннях цифровий ключ, маскуючи його в кінці документу. Зокрема, цифровий ключ „1243” був внесений в кінці одного з вилучених співробітниками МДБ документів УПА, як „1243 рік”, тобто його було замасковано під помилку у даті<sup>34</sup>.

Схожі цифрові ключі застосовувалися керівниками підпілля ОУН під час листування між собою для шифрування дат зустрічей, справжніх прізвищ і т.п. цінної інформації. Це стало відомо з їх свідчень після арешту органами держбезпеки УРСР.

Наприклад, керівник ОУН в Україні і головний командир УПА у 1950-1954 рр. Василь Кук – „Леміш” для текстових повідомлень використовував цифровий ключ „735281”, для шифрування дат зустрічей – ключ „251015”, а для зашифрування цифр літерами – слово „Ульяновськ”.

Член проводу ОУН в Україні і керівник крайового проводу ОУН на Північно-західних українських землях Василь Галаса – „Орлан” для шифрування тексту застосовував 15 аркуш брошури ОУН „Радянський патріотизм”, рядки відраховував згори донизу. Для зашифрування дат зустрічей В. Галаса використовував цифровий ключ „487294”.

Член крайового проводу ОУН на Північно-західних українських землях „Ат” для зашифрування текстів використовував ключ „Дуничка”. Цей же ключ він переводив на цифровий за українським алфавітом (5 – 23 – 17 – 10 –

27 – 14 – 1), і використовував так, як було вказано вище. Ключем для шифрування цифр було слово „куропатнічев”, для шифрування дат – число „121806”<sup>35</sup>.

#### **Д) Шифрування за допомогою заміни літер на інші символи.**

Окрім вказаних вище способів, підпільниками ОУН застосовувався і такий спосіб, як заміна одних літер на інші символи та знаки.

В цьому випадку всі літери українського алфавіту довільно замінялися на інші літери та символи: наприклад, „к” – на „а”, „і” – на „о”, „н” – на „р”, „о” на „б” і т.д.

В такому випадку, якщо підпільникам потрібно було зашифрувати слово „кіно”, в результаті вийде нічого не означаюча для стороннього ока підбірка літер „аорб”.

На думку співробітників МДБ, такий спосіб доволі легко піддавався розшифруванню, оскільки кожній букві відповідає лише одне умовне позначення. Проаналізувавши текст, можна було відшукати подвійні літери в словах (наприклад „нн”), часто вживані закінчення, префікси, певні повторення і т.п.

До цього ж способу зашифрування відносились і заміна літер українського алфавіту на умовні символи та знаки, які вживалися у фізиці та математиці тощо. При такому способі зашифровані літери могли мати наступний вигляд: „а” – „+”, „б” – „=”, „в” – „№”, „г” – „%” і т.д.

Шифрування за допомогою заміни літер на інші символи у підпіллі ОУН і УПА застосовувалося дуже часто. Хоча підпільники розуміли, що вказаний спосіб простіше дешифрувати, аніж цифрове шифрування або використання шифрувальних квадратів, вони все одно постійно використовували його. Думається, що учасників ОУН і УПА приваблювала простота та швидкість написання документації під час застосування цього методу.

Органами державної безпеки УРСР неодноразово розшифровувалися подібні тексти. Розглянемо конкретний приклад. Перед травневими святами 1954 р. невідомими особами було порізано 8 державних прапорів СРСР та 6 портретів керівників КПРС і уряду, які були виставлені біля трибуни у місті Володимир-Волинській Волинської області.

Тривалий час органам КДБ не вдавалося з’ясувати, хто ж зумів здійснити цю акцію. Під час розшуку було виявлено низку осіб, які викликали підозру, однак впевненості, чи саме вони порізали прапори і портрети – не було.

У числі інших заходів під час розшуку співробітники КДБ потаємно перевіряли листи, які направлялися мешканцями м. Володимир-Волинський до своїх рідних та знайомих у різні міста СРСР. У вересні 1954 р. вони перехопили документ, який йшов на адресу червоноармійця Степана Фуга. У цьому листі було виявлено групи літер, які не мали смислової інформації.

Співробітники КДБ запідозрили, що це було зашифроване послання, в якому справжні літери були замінені на інші символи.

В результаті розшифровки засекреченого тексту було встановлено, що у м. Володимир-Володимирський тривалий час діяла молодіжна група ОУН. Її учасники у листі звітували С. Фузі про виконану роботу, зокрема про знищення радянської символіки на початку травня 1954 р., і повідомляли, що обласне управління КДБ поки що про на їх слід не натрапило і про обставини акції нічого не знає.

Цей лист був зашифрований самим простим способом: одні літери були замінені на інші: „а” – на „р”, „б” на „и”, „в” – на „с”, „ж” – на „у”, „і” на „к” і т.д.

В результаті розслідування було встановлено всіх учасників молодіжної ланки ОУН, якою керував С. Фуга. Частина з них було заарештовано та засуджено, а з решту використано у якості свідків<sup>36</sup>.

Методика розшифрування органами держбезпеки таких документів нічим не відрізнялося від попередніх.

### Е) Шифрувальна решітка.

Найскладнішою системою написання підпільної документації, яка практично не піддавалася розшифруванню, було використання так званої шифрувальної решітки. Її переважно застосовували керівники підпілля.

Цю решітку малювали на звичайному папері або ж на картоні. Збоку вона виглядала, як розбитий на клітки квадрат, у якому в окремих місцях були вирізані „вікна”. Вона могла мати приблизно такий вигляд:

*				*			
		*					*
				*			
	*					*	
*		*		*			
					*		*
		*				*	
	*				*		

Помічені символом „\*” клітки підпільниками вирізалися, а взагалі кількість кліток могла бути довільною (зазвичай від 7 на 7 до 10 на 10).

Ця решітка застосовувалася наступним чином: її клали на папір і крізь вирізані „вікна” учасники ОУН послідовно записували по одній літері (або по

одному складу слова) текст, який підлягав зашифруванню. Коли всі „вікна” заповнювалися, то решітка переверталася на 90 градусів вправо і текст вносився знову. Ця процедура повторювалася 4 рази.

„Вікна” у квадраті вирізалися таким чином, щоб при повертанні 4 рази вони завжди потрапляли на чисте місце.

Якщо після цього залишався не зашифрований текст, то решітку клали на чисте місце на папері і повторювали ту ж саму процедуру знову. Коли текст послання був повністю зашифрований, а чисті „вікна” все ще залишалися, то їх заповнювали довільними літерами.

Текст, зашифрований за допомогою шифрувальної решітки, можна було легко відрізнити від текстів, зашифрованих іншими способами: він завжди мав однакову кількість рядків по вертикалі та горизонталі і виглядав збоку, як квадрат, наповнений літерами. Однак розшифрувати його було майже неможливо, оскільки використовуючи квадрат із 64 клітин (8 на 8) можна було скласти понад 10 тисяч різних варіантів. Не знаючи, які саме клітини в квадраті були вирізані, не було можливості зачепитись за будь-які особливості тексту. Тому розшифрування такого тексту співробітниками МДБ проводилося навздогад<sup>37</sup>.

### 3. ТАЙНОПИС

Окремо від кодів та шифрів слід розглянути застосування у підпіллі ОУН тайнопису. Під ним слід розуміти використання автором документації спеціальних чорнил, виготовлених таким чином, щоб після написання інформації на папір ніхто не те, що не міг прочитати написаного, а й взагалі здогадатися, що тут щось написано.

Учасниками ОУН для тайнопису використовувалися найрізноманітніші чорнила: починаючи від самого звичайного молока, яке проявлялося внаслідок нагрівання паперу над вогнем, і закінчуючи складними хімічними сполуками, які практично неможливо було виявити.

Зазвичай підпільники писали тайнописом текст, не зашифровуючи його за допомогою кодів та шифрів, оскільки „специфічні” чорнила були найкращим способом захистити важливу інформацію від чужого ока.

5 березня 1950 р. в с. Білогорща біля м Львів був вбитий Головний командир УПА та керівник Проводу ОУН в Україні Роман Шухевич – „Тарас Чупринка”. Під час обшуку у його криївці співробітниками МДБ було вилучено значний обсяг документів та речей, серед яких – спеціальні таблетки і реактиви, призначені для тайнопису та інструкція щодо їх використання. Ймовірно всі ці засоби Р.Шухевич отримав з-за кордону.

У інструкції зазначалося, що для приготування спеціального чорнила потрібно було розчинити одну таблетку у певній кількості якісного алкоголю. Таблетку спочатку рекомендувалося розкришити рукою на дрібні шматки, а потім цілковито розтерти у великій ложці за допомогою чайної ложечки. Після зсипання розтертої таблетки до алкоголю розтерта таблетка

повільно розчинялася протягом кількох хвилин, при цьому рекомендувалося розтрусати суміш, аж поки порошок цілковито не розчиниться.

Надзвичайно важливим було правильно підібрати алкоголь, щоб він був чистим і мав високий процент спирту. Рекомендувалося спочатку написати самим алкоголем на папері текст, потім висушити його гарячим залізом аж до припалювання і перевірити, чи не просвітлюється текст. Якщо можна було розібрати зміст написаного, то це означало, що алкоголь був не зовсім чистий і має складники, небажані для таємного письма. У інструкції рекомендувалося використовувати джин або горілку, хоча і вони не завжди себе виправдовували.

Коли чорнила були приготовані, підпільники розпочинали писати текст Приладом для написання був загострений з одного боку патичок або сірник чи паличка для чищення зубів. Підпільники слідкували, щоб патичок не дряпав папір під час написання слів.

Після написання тексту (наприклад – між рядками звичайної книги) непосвячені люди навіть не могли здогадатися про його наявність. Виявити такий текст можна було лише за допомогою спеціального хімічного проявника<sup>38</sup>.

Окрім того, підпільники ОУН використовували і інші способи шифрування документів, але вони рідко застосовувалися у практичній роботі. Найбільш часто вживані способи наведені вище.

## ВИСНОВКИ

Підсумовуючи викладене слід відзначити, що використання шифрів та кодів а також вміле зашифрування документів дійсно допомагало учасникам ОУН і УПА передавати та зберігати особливо важливу інформацію. Якщо у боях гинули люди, особливо – керівники, і у них вилучали зашифровані документи, то ці записи не давали змогу чекістам швидко проводити оперативні заходи, щоб одразу ж розгромити організаційні ланки підпілля. Чимало документів ОУН, вилучених у вбитих підпільників та у їх сховищах, так і залишилися нерозшифрованими. Можливо це стало однією із причин того, що організована боротьба ОУН із радянською владою тривала так довго, аж до середини 1950-х років.

Використання підпіллям ОУН шифрів та кодів є цікавим прикладом застосування конспіративних методів у листуванні. У нашій праці наведено лише окремі приклади застосування кодів та шифрів. Сподіваємося, що вона допоможе зацікавленим дослідникам краще зрозуміти принципи роботи з подібними шифрувальними методами і сприятиме у подальшому вивченню діяльності українського національно-визвольного руху, адже в архівах України і досі зберігаються сотні зашифрованих документів ОУН і УПА.

З іншого боку слід відзначити, що використання шифрів та кодів несло для підпільної організації значну небезпеку. Органами державної безпеки УРСР неодноразово вилучалися особисті блокноти керівників ОУН і УПА, в

яких містилися не лише зашифровані документи, але й самі коди та шифри, використовуючи які можна було розшифрувати захоплені матеріали. Розшифрувавши документацію співробітники МДБ мали змогу проводити успішні заходи проти підпілля. Особливо небезпечним для підпілля було розшифрування списків його учасників та прихильників, домовлених місць зустрічей тощо.

28 листопада 1950 р. співробітники органів МДБ в бункері біля с. Велике Поле Івано-Франківського району Львівської області вбили керівника Львівського крайового проводу ОУН Осипа Дяківа – „Горнового”. У бункері були виявлені кілька його особистих блокнотів та записи, які він не встиг знищити. Серед них були два коди для зв'язку між керівниками підпілля ОУН в Україні, кілька паролів для зустрічей, статистичні дані про учасників ОУН на території Львівської області та інші документи<sup>39</sup>. Шифрувальна таблиця, яку використовував О. Дяків, мала в основі слово „генчупринка” і виглядала так:

	1	2	3	4	5	6	7	8	9	10	11
1	Г	Е	Н	Ч	У	П	Р	И	Н	К	А
2	Д	Є	О	Ш	Ф	Р	С	Й	О	Л	Б
3	Е	Ж	П	Щ	Х	С	Т	К	П	М	В
4	Є	З	Р	Ю	Ц	Т	У	Л	Р	Н	Г
5	Ж	І	С	Я	Ч	У	Ф	М	С	О	Д
6	З	Ї	Т	Ь	Ш	Ф	Х	Н	Т	П	Е
7	І	И	У	А	Щ	Х	Ц	О	У	Р	Є
8	Ї	Й	Ф	Б	Ю	Ц	Ч	П	Ф	С	Ж
9	И	К	Х	В	Я	Ч	Ш	Р	Х	Т	З
10	Й	Л	Ц	Г	Ь	Ш	Щ	С	Ц	У	І
11	К	М	Ч	Д	А	Щ	Ю	Т	Ч	Ф	Ї

Таким чином, у разі виявлення документів підпільників, які підтримували зв'язок з О. Дяковим, органи МДБ могли одразу ж розшифрувати вилучене листування.

Інший приклад пов'язаний з Головним командиром УПА Романом Шухевичем, який загинув 5 березня 1950 р. в с. Білогорща біля Львова. Співробітниками МДБ у його сховищі було вилучено блокнот, де виявилися записи про зустрічі між керівниками ОУН, обумовленими на весну 1950 р. Вони свідчили про те, що зустрічі між зв'язковим Р. Шухевича та одного з керівників підпілля під цифровим псевдонімом „99” повинні були відбутися в 10 годин ранку 24 квітня та 2 травня 1950 р. на дорозі з м. Болехів у с. Гошів. Запасні зустрічі на непередбачувані випадки були призначені на 6 та 11 травня 1950 р. на вул. Задвірнянській з 18 до 18.15, але в якому місті – вказано не було. Окрім того, у блокноті Р. Шухевича було вказано прикмети зв'язкової П. Федуна для запасної зустрічі: на голові – синя хустина, в лівій руці – солом'яна корзина. Вказувалися також паролі для зв'язку:



Зв'язкова від „99”: „Де тут є залізний склеп?”

Зв'язкова Р. Шухевича: „Тут немає залізного склепу, тільки цукорня”.

Таким чином, у співробітників МДБ в руках опинилися виходи на діючі лінії підпільного зв'язку. Порушення правил конспірації Головним командиром УПА Р. Шухевичем щодо дотримання у таємниці місць та обумовленостей зустрічей зв'язкових згодом принесли для підпілля погані наслідки.

О 10 годин ранку 24 квітня та 2 травня 1950 р. на дорозі з м. Болахів у с. Гошів органами МДБ було встановлено приховане спостереження, однак зв'язкові П. Федуна та Р. Шухевича на заплановану зустріч так і не з'явилися.

У зв'язку з цим було вжито заходів до захоплення зв'язкових ОУН на зустрічах 6 та 11 травня 1950 р. Як виявилось, вулиця Задвірнянська була у двох містах: Львові та Станіславі. У зв'язку з цим було створено дві спеціальні групи МДБ, якими 6 травня 1950 р. було встановлено приховане спостереження за місцями зустрічей. Туди ж були направлені співробітники МДБ, які знали по фотографіям членів та зв'язкових Проводу ОУН в Україні.

Однією з таких груп співробітників МДБ за вказаними у блокноті Р. Шухевича прикметами на вул. Задвірнянській у Львові була впізнана, затримана та заарештована зв'язкова проводу ОУН в Україні Голояд Галина Омелянівна – „Марта”, 1922 р.н., ур. м. Львів. Під час обшуку у неї виявили листи від П. Федуна до Р. Шухевича та інших керівників ОУН, велику кількість інформативних та пропагандистських документів, пістолет „Вальтер” та дві обійми набоїв до нього<sup>40</sup>.

Під час допитів в УМДБ по Львівській області Г. Голояд вимушена була зізнатися, що з жовтня 1949 р. до травня 1950 р. виконувала функції технічної співробітниці референтури пропаганди Проводу ОУН в Україні. Весь цей час вона переховувалася з П. Федуном в бункері керівника Долинського надрайонного проводу ОУН Ярослава Зборика – „Арсена”, який, по суті, виконував обов'язки керівника лінії зв'язку від П. Федуна до керівників Карпатського крайового проводу ОУН. Г. Голояд виконувала вибірку матеріалів зі звітів ОУН, які надходили до П. Федуна та літературно опрацьовувала їх з метою подальшого опублікування в підпільній пресі. Крім того, вона написала статті та вірші патріотичного змісту, які органами МДБ вважалися антирадянськими та націоналістичними. 29 квітня 1950 р. П. Федун направив Г. Голояд у м. Львів на зустріч зі зв'язковою Р. Шухевича. Після виконання доручення вона повинна була в іншому місці зустрітися з зв'язковими О. Дяківа, а потім повернутися до П. Федуна в Карпати.

Під тиском слідчих Г. Голояд вимушена була назвати відомі їй орієнтири, за якими можна було розшукати місцезнаходження бункера Я. Зборика у лісі біля с. Ілемня Рожнятівського району Станіславської області. В результаті 14 травня 1950 р. Я. Зборик та його дружина „Леся” були виявлені та заарештовані, а П. Федуну ледве пощастило уникнути переслідування і втекти<sup>41</sup>.

Слід сказати, що своєчасній та точній розшифровці документів ОУН і УПА, які потрапляли до органів держбезпеки УРСР, надавалося серйозне значення. В управлінні 2-Н в м. Києві та відділах 2-Н обласних управлінь МДБ УРСР працювали досвідчені співробітники, які неодноразово успішно розшифровували важливі підпільні документи. У матеріалах ГДА СБ України збереглися окремі приклади успішного використання співробітникам МДБ розшифрованих документів у розгромі ланок ОУН. Розглянемо один із них.

Оперативна група УМДБ по Волинській області в жовтні 1951 р. розшукувала керівника Луцького окружного проводу ОУН Олександра Савиру – „Яроша”. У жовтні 1951 р. у Берестечківському районі Волинської області вона знайшла бункер ОУН, з якого конфіскувала чималу кількість підпільної літератури та записів керівників. З них кілька аркушів було зашифровано.

В процесі тривалого процесу розшифрування оперативниками було встановлено, що шифрування було здійснене за четвертим аркушем брошури ОУН „Вказівки батькам у вихованні дітей”, рядки читалися згори донизу, літери зліва направо, цифри шифрувалися словом „дніпрогеса”.

Розшифрований список виявився переліком особливо довірених зв'язкових та симпатиків підпілля. У ньому вказувалися села та райони їх проживання, дійсні та запасні паролі тощо. Органи МДБ встановили стеження за всіма цими особами.

В результаті вказаних заходів 3 грудня 1951 р. спостерігачами МДБ було помічено, що до одного із прихильників ОУН в будинок поспіхом зайшли двоє невідомих молодих хлопців. Одразу ж була викликана чекістсько-військова група, яка знаходилась неподалік. Після прибуття та блокування будинку вона була обстріляна і зав'язала бій з підпільниками, які заховалися на даху. Під час тривалого бою з чекістами загинув керівник Берестечківського районного проводу ОУН „Сизон” (або „Сазон”, „Сезон”) та був захоплений живим його бойовик „Матвій”. З вилучених у них документів стало відомо про місця укриття боївки Луцького окружного проводу ОУН та прізвища багатьох прихильників ОУН у різних селах області<sup>42</sup>.

Підсумовуючи наше дослідження, хочеться висловити сподівання на те, що у майбутньому до вивчення шифрів та кодів ОУН і УПА долучаться і молоді науковці, зокрема ті, які згодом працюватимуть в Українському інституті національної пам'яті, створеному за розпорядженням Президента України.

За Українську Самостійну  
Соборну Державу!

Воля народам! Воля людині!

## ПОНЕВОЛЕНИЙ УКРАЇНСЬКИЙ НАРОДЕ!

жувати чи знищувати большевизькі магазини,  
знищувати хліб, призначений на хлібоздачу  
державі. Саботаж стосувався на фабриках і за-  
водах, у шахтах, на транспорті, в колгоспах, у  
всіх установах. Таким чином ми будемо над-  
шарпувати економічну міць ворога — (дну з  
найважливіших) підстав його сили. Тихий інди-  
відуальний саботаж — це засіб боротьби, дос-  
тупний для кожного українця й українки. Він  
повинен бути відважно і широко стосований.  
Хай не вдаються ворогові його вплив еконо-  
мічної експлуатації України й українського  
народу. Хай не вдаються ворогові його плани  
розбудови воєнної моці. Хай з трупицями  
вдається йому свати з України і багатства.

7. Таємно знищувати найзапекліших  
большевизьких вислужників з мвд мго, з  
адміністрації, сексотів, найзапекліших ру-  
сифікаторів України з-поміж росіян.

8. Шукати революційну літературу україн-  
ського підпільного визвольного руху, читати  
видання ОУН і УПА, поширювати їх у відпи-  
сах між своїми добрими знайомими. Листівки  
і заклики переписувати, хоч би навіть рукою  
і таємно їх розповсюджувати в населених пун-  
ктах, по школах, у кінотеатрах тощо. Викону-  
вати всі заклики і вказівки ОУН. Бути кожно-  
часно готовим, щоб, коли прийде для цього  
сприятлива нагода, на поклик ОУН під керів-  
ництвом С.Бандери зброєю у руках стану-  
ти до остаточної збройної розправи з москов-  
сько-большевизькими окупантами України.

1 9 5 0

— 8 —

Брошура ОУН „Поневолений український народ!”, за 8 сторінкою якої був зашифрований список прихильників ОУН. В тексті видно розмежування.

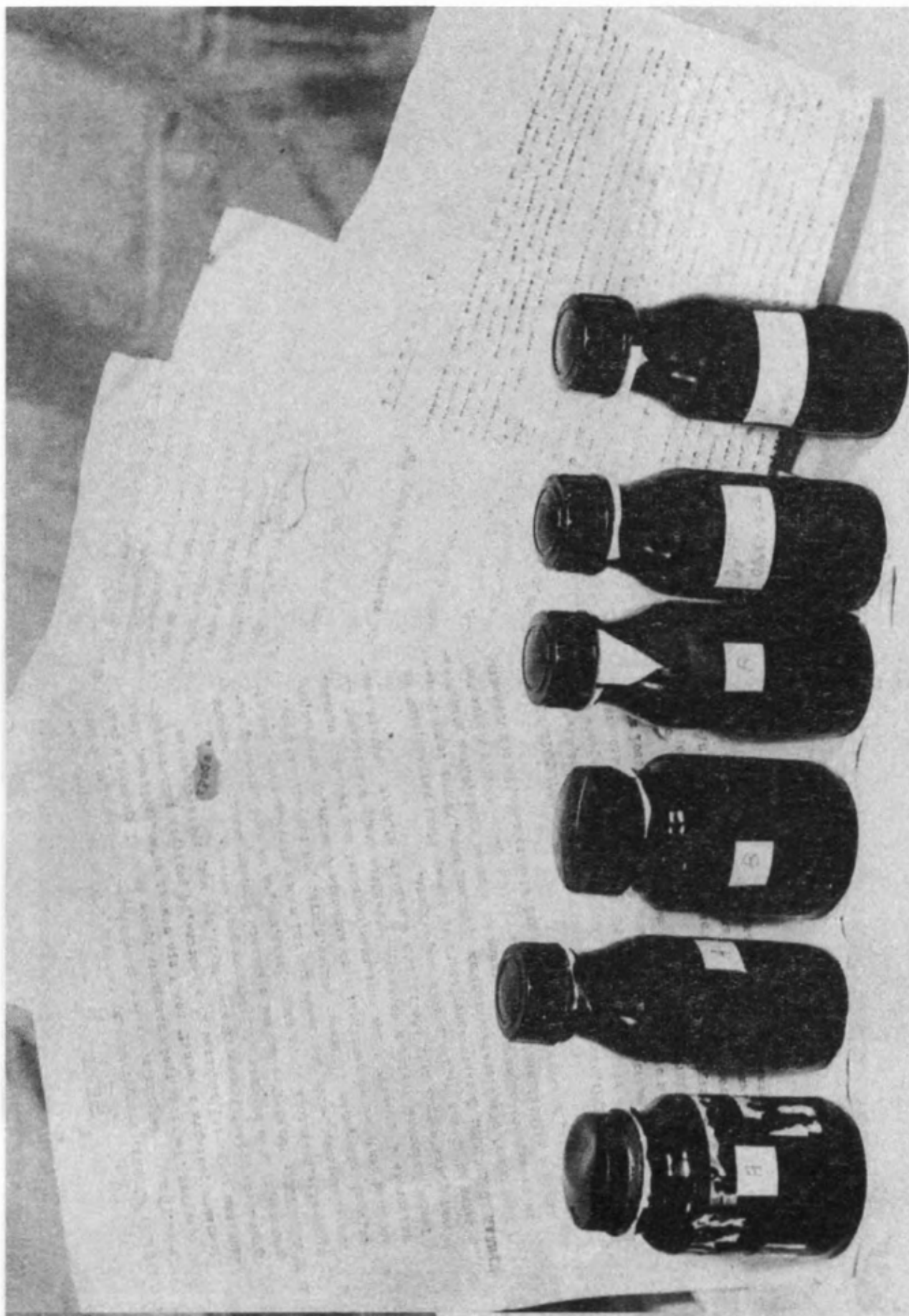


Пошта, яка направлялася в адресу члена Проводу ОУН в Україні  
Петра Федуна – „Петра Полтави”.  
Він використовував цифровий псевдонім „99”.



Головний командир УПА та керівник ОУН в Україні в 1943-1950 рр.  
 Роман Шухевич  
 та керівник Львівського проводу ОУН в 1948-1950 рр. Осип Дяків – „Наум”.





Засоби тайнопису, вилучені у криївці Р. Шухевича 5 березня 1950 р.





**Олександр Савира – „Ярош”. Керівник Луцького окружного проводу ОУН.  
Загинув 14 травня 1953 р.**



**Зв'язкові В. Кука йдуть в лісі. 1 – Володимир Кілярський - „Дем'ян”,  
2 – Василь Кузів - „Орач”, 3 – Василь Порплиця - „Байда”, 4 – „Довбуш”,  
5 – Михайло Заєць - „Зенко”, 6 – „Петро”.**





Незважаючи на суворі правила конспірації – життя брало своє. Керівник Львівського крайового проводу ОУН Зиновій Тершаковець – „Федір” пригощає підпільників ОУН шампанським з нагоди одного із свят.

1 – „Федір”, 2 – Ярослав Дякон - „Мирон”, 3 – „Тарапон”  
4 – „Скалка”, 5 – „Світовий”, 6 – „Петро”.



Керівник Львівського крайового проводу ОУН Осип Дяків – „Цьвочок”  
зачитує підлеглим наказ.

1 – „Петро”, 2 – „Явір”, 3 – „Чабан”, 4 – „Крук”, 6 – Любомира Гаєвська –  
„Рута”, 7 – Осип Дяків – „Цьвочок”.



Керівник Долинського надрайонного проводу ОУН  
Ярослав Зборик – „Арсен” та його дружина „Леся”.



Керівник реферетури пропаганди Проводу ОУН в Україні  
Петро Федун – „Петро Полтава” та його зв’язкова Галина Голояд – „Марта”.

- <sup>1</sup> Галузевий державний архів Служби безпеки України (далі – ДА СБ України). – Ф 13. – Спр. 376 – Т 59 – Арк. 1-31, 32-46; Спр 372. – Т. 17. – Арк. 1-66, 67-90, 111-120, 121-123, 124-130.
- <sup>2</sup> Там само. – Спр. 376. – Т. 59 – Арк. 67-73.
- <sup>3</sup> Там само. – Арк. 98-100; Спр. 372. – Т. 17 – Арк. 245-246
- <sup>4</sup> Там само. – Спр. 376. – Т. 59 – Арк. 105
- <sup>5</sup> Там само. – Арк. 134-151; Спр 372. – Т. 17 – Арк. 91-110.
- <sup>6</sup> Там само – Спр 376. – Т 59 – Арк 152-155
- <sup>7</sup> Там само. – Арк. 81-97.
- <sup>8</sup> Там само – Арк 101-104
- <sup>9</sup> Див. інструкції „Короткі вказівки до конспірації підпільника”, „Застереження”, „Кілька пригадок щодо побуту підпільника”, „Конспіративні вказівки стосовно друзів”, „Додаткові вказівки з питань конспірації” і т.д // Там само. – Спр. 372. – Т. 17 – Арк. 257-266, 267-270, 278-284, 285-290, 299-310
- <sup>10</sup> Там само Спр 376 – Т 59. – Арк 156-189, 190-197.
- <sup>11</sup> Наприклад, див. розділ „Шифр і код” у брошурі „Конспірація” // Там само. – Спр 372 – Т 17. – Арк. 50-62
- <sup>12</sup> Там само. – Спр. 376 – Т. 59 Арк 74-78.
- <sup>13</sup> Там само. – Арк 79
- <sup>14</sup> Див.. Там само. В томі № 59 з справи № 376 містяться різні видання ОУН щодо дотримання конспірації, в т.ч. і про застосування шифрів та кодів.
- <sup>15</sup> Р. Петренко Спогади / Літопис УПА. – Львів Торонто, 1997. – Т. 27
- <sup>16</sup> М. Савчин. Тисяча доріг Спогади / Літопис УПА. – Львів –Торонто, 1995. – Т. 28 – 600 с
- <sup>17</sup> Русначенко А М. Народ збурений Національно-визвольний рух в Україні й національні рухи опору в Білорусії, Литві, Латвії, Естонії у 1940-50-х роках. – К.: Унів. вид-во „Пульсари”, 2002. – 401 с.
- <sup>18</sup> Кентій А В. Нарис боротьби ОУН-УПА в Україні (1946-1956 рр.) / Інститут історії України НАН України. - К., 1999. - 111с.
- <sup>19</sup> Сергійчук В Український здви́г – Київ, 2004-2005. – Т. 1-5.
- <sup>20</sup> Всденєєв Д. Організаційна еволюція Служби безпеки ОУН (С. Бандери) (1939-початок 1950-х років) // Наукові записки: Збірник наукових статей Національного педагогічного університету імені М.П. Драгоманова / Укл. П.В.Дмитренко, Л.Л.Макаренко – К.: НПУ, 2001. – Випуск 44 – С 188-194; Його ж: Контррозвідувальне забезпечення в Українській повстанській армії // Сторінки воєнної історії України: Збірник наукових праць. Вип. 4 / Відп. ред. В.А. Смолій. – К : Інститут історії України НАН України, 2000. – С 166-170; Його ж: До питання про тактику дій підпілля ОУН (друга половина 1940-х - початок 1950-х років) // Проблеми історії України: факти, судження, пошуки: Міжвідомчий збірник наукових праць Вип. 6 / Відп. ред. В.А. Смолій. — К.: Інститут історії України НАН України, 2002. – С. 449-457; Його ж: Меч і тризуб. Нотатки до історії Служби безпеки Організації українських націоналістів // 3 архівів ВУЧК-ГПУ-НКВД-КГБ. – 1998. – № 1/2. – С. 365-389; 2000. – № 2/4. – С. 485-503 (співавтор - Єгоров В.).
- <sup>21</sup> Див.. Здіорук (Стельмах) О.І. Літопис УПА: час, події, джерела: (Джерелознавча достовірність та інформаційна цінність багатотомного видання "Літопис УПА") – К.: Інститут історії України НАН України, 2000. – 142 с
- <sup>22</sup> Див.: Літопис УПА. – Київ-Торонто, 2006. – Т. 8. – 1450 с.
- <sup>23</sup> ДА СБ України. – Ф. 13. – Спр. 372. – Т 53. – Арк. 242.
- <sup>24</sup> Там само. – Т. 87 – Арк. 269.
- <sup>25</sup> Там само. – Арк. 280-282.
- <sup>26</sup> Там само. – Арк. 283

- 
- <sup>27</sup> Там само. – Т. 19. – Арк. 48.  
<sup>28</sup> Там само. – Т. 87. – Арк. 284.  
<sup>29</sup> Там само. – Арк. 286-287.  
<sup>30</sup> Там само. – Арк. 288.  
<sup>31</sup> Там само. – Т. 19. – Арк. 8-9.  
<sup>32</sup> Там само. – Т. 87. – Арк. 289-292.  
<sup>33</sup> Там само. – Арк. 293-294.  
<sup>34</sup> Там само. – Т. 19. – Арк. 1-2.  
<sup>35</sup> Там само. – Т. 87. – Арк. 294-295.  
<sup>36</sup> Там само. – Арк. 297-305.  
<sup>37</sup> Там само. – Арк. 296-297.  
<sup>38</sup> Там само. – Спр. 398. – Т. 12. – Арк. 20, пакет.  
<sup>39</sup> Там само. – Спр. 372. – Т. 18. – Арк. 210-245, Т. 19. – Арк. 66-68.  
<sup>40</sup> Там само. – Т. 88. – Арк. 220-221.  
<sup>41</sup> Там само. – Ф. 11. – Спр. С-9112. – Т. 3. – Арк. 216-230.  
<sup>42</sup> Там само. – Т. 87. – Арк. 296-305.